

Express Mail Label No.

Dated: _____

Docket No.: 20046/0200694-US0
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Gernot Eckstein et al.

Application No.: 10/735,517

Confirmation No.:

Filed: December 11, 2003

Art Unit: N/A

For: PREVENTING THE UNWANTED
EXTERNAL DETECTION OF OPERATIONS
IN DIGITAL INTEGRATED CIRCUITS

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:


Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Germany	101 28 573.6	June 13, 2001

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: February 2, 2004

Respectfully submitted,

By  ^{Reg. No. 53,175}
Laura C. Brutman

Registration No.: 38,395
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 753-6237 (Fax)
Attorneys/Agents For Applicant

BUNDESREPUBLIK DEUTSCHLAND



Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 101 28 573.6

Anmeldetag: 13. Juni 2001

Anmelder/Inhaber: Infineon Technologies AG,
München/DE

Bezeichnung: Verhindern der unerwünschten externen Erfassung
von Operationen in integrierten Digitalschaltungen

IPC: H 04 L, G 06 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 09. Januar 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

A handwritten signature in black ink, consisting of a stylized 'H' followed by a horizontal line.

Holb.

Patentanwälte · Postfach 710867 · 81458 München

Infineon Technologies AG

St.-Martin-Str. 53

81669 München

PATENTANWÄLTE

European Patent Attorneys
European Trademark Attorneys

Fritz Schoppe, Dipl.-Ing.
Tankred Zimmermann, Dipl.-Ing.
Ferdinand Stöckeler, Dipl.-Ing.
Franz Zinkler, Dipl.-Ing.

Telefon/Telephone 089/790445-0
Telefax/Facsimile 089/790 22 15
Telefax/Facsimile 089/74996977

e-mail: szsz_iplaw@t-online.de

**Verhindern der unerwünschten externen Erfassung von Operationen
in integrierten Digitalschaltungen**

Beschreibung

Verhindern der unerwünschten externen Erfassung von Operationen in integrierten Digitalschaltungen

5

Die vorliegende Erfindung befaßt sich mit einem Verfahren zum Verhindern des externen Erfassens von Operationen in einer integrierten Digitalschaltung sowie mit einer integrierten Digitalschaltung, bei der das unerwünschte externe Erfassen von Operationen innerhalb der integrierten Digitalschaltung verhindert wird. Insbesondere befaßt sich die vorliegende Erfindung mit einer Gegenmaßnahme gegen sogenannte Side-Channel-Attacken, wie sie zum Zweck der Analyse von integrierten Digitalschaltung durchgeführt werden.

15

Bei vielen integrierten Digitalschaltungen muß verhindert werden, daß deren Betriebsweise von unberechtigten Personen analysiert wird. Beispielhafte Schaltungen, bei denen derartige Angriffsszenarien abzuwehren sind, sind Chipkarten-ICs, Sicherheits-ICs oder auch einzelne Schaltungsmodul derartiger ICs, wie beispielsweise Kryptocoprozessoren. Es bedarf keiner Erläuterung, daß es verhindert werden muß, daß unberechtigte Personen die von einem Kryptocoprozessor durchgeführten Verschlüsselungsalgorithmen analysiert.

25

Typischen Angriffsszenarien, mit denen unberechtigte Personen versuchen, beispielsweise die von einem Kryptocoprozessor ausgeführten Verschlüsselungsalgorithmen zu analysieren, werden als sogenannte Side-Channel-Attacken bezeichnet. Derartige Side-Channel-Attacken umfassen beispielsweise die differenzielle Leistungsaufnahmeanalyse (DPA = differential power analysis), die Erfassung der elektromagnetischen Abstrahlung des betreffenden ICs oder sogenannte Timing-Attacken.

30

Im Gegensatz zu synchronen Schaltungen haben asynchrone Schaltungen, zu denen auch selbst-zeitgebende Schaltungen (self-timed Schaltungen) zählen, die vorteilhafte Eigen-

35

schaft, daß ihre Verarbeitung nicht mit einem zeitlich periodischen Ereignis, wie dem Takt, direkt korreliert ist. Daher zeigt ihre Verarbeitung auch keine Abhängigkeit von einem derartigen zeitlich-periodischen Ereignis, wodurch es bei den asynchronen Schaltungen schwieriger ist, erfolgreiche Side-Channel-Attacken durchzuführen. Jedoch hängt auch bei asynchronen Schaltungen im allgemeinen die Zahl der schaltenden Elemente von der speziellen, zu verarbeitenden Operation ab, so daß generell Datenabhängigkeiten der Verarbeitung auftreten, die sich im Profil der Stromaufnahme der betreffenden Schaltung wieder erkennen lassen.

Um derartige Attacken zu erschweren, ist es bekannt, in den Verarbeitungsablauf sogenannte Random-Wait-States also zufällige Wartezustände einzufügen. Ebenfalls ist es bekannt, Unterbrechungen der Ausführung von Operationen in der CPU zu erzwingen. Bei der Einfügung der Random-Wait-States sind mögliche Variationen des zeitlichen Ablaufs der Operationen begrenzt, da nicht zu jedem beliebigen Zeitpunkt eine Verzögerung aktiviert werden kann bzw. ein Wartezustand eingefügt werden kann. Auch die Maßnahme der Unterbrechung in der Ausführung in der CPU kann die Side-Channel-Attacken nicht vollständig abwehren, da sich derartige Unterbrechungen durch die veränderte Stromaufnahme erfassen lassen.

Ausgehend von diesem Stand der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein Verfahren zum Verhindern des externen Erfassens von Operationen in einer integrierten Digitalschaltung, die eine asynchrone Schaltung aufweist, zu schaffen.

Ferner liegt der Erfindung die Aufgabe zugrunde, eine integrierte Digitalschaltung, die eine asynchrone Schaltung hat, so weiterzubilden, daß das unerwünschte externe Erfassen von Operationen in der Digitalschaltung verhindert wird.

Die erstgenannte Aufgabe wird durch ein Verfahren nach Anspruch 1 gelöst.

5 die zweitgenannte Aufgabe wird durch eine integrierte Schaltung nach Anspruch 3 gelöst.

Die Erfindung schafft ein Verfahren zum Verhindern des externen Erfassens von Operationen in eine integrierte Schaltung, die eine asynchrone Schaltung aufweist, mit dem Verfahrensschritt des zeitlichen Veränderns einer Versorgungsspannung der asynchronen Schaltung, um den Ausführungszeitpunkt von Operationen innerhalb der asynchronen Schaltung zeitlich zu verschieben. Bei einem bevorzugten Aspekt der Erfindung erfolgt die Veränderung der Versorgungsspannung in zufälliger Weise.

10
15

Der Erfindung liegt die Erkenntnis zugrunde, daß durch Überlagerung eines zufallsgesteuerten, also unvorhersehbaren zeitlichen Jitters über die Versorgungsspannung ein zufälliger zeitlicher Jitter bei den Ausführungszeiten der Operationen erreicht wird, wodurch ein Aufsynchronisieren der Einzelmessungen bei den Side-Channel-Attacken verhindert wird. Der zeitliche Jitter bei der Ausführung der Operationen innerhalb der asynchronen Schaltung führt jedoch nicht Verarbeitungsfehlern, da asynchrone Schaltungen ihrer Natur nach eine Selbstsynchronisation bewirken.

20
25

Gemäß einem Vorrichtungsaspekt der Erfindung umfaßt die integrierte Digitalschaltung eine asynchrone Schaltung und eine Einrichtung zum zeitlichen Verändern der Versorgungsspannung, mit der die asynchrone Schaltung versorgt wird, wodurch der Ausführungszeitpunkt von Operationen innerhalb der asynchronen Schaltung zeitlich verschoben wird.

30

35 Nachfolgend wird ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung unter Bezugnahme auf die beiliegende Zeichnung näher erläutert. Es zeigt:

Die einzige Figur ein Blockdiagramm einer integrierten Digitalschaltung gemäß einem bevorzugten Ausführungsbeispiel der Erfindung.

5

Die erfindungsgemäße integrierte Digitalschaltung, die in ihrer Gesamtheit mit dem Bezugszeichen 1 bezeichnet ist, umfaßt eine asynchrone Schaltung 2, eine Generatorschaltung 3 zum Erzeugen tatsächlicher Zufallszahlen (true random number generator), einen Digital/Analog-Wandler 4, dem eingangsseitig die von der Generatorschaltung erzeugten digitalen Zufallszahlen zugeführt werden und der ausgangsseitig einen entsprechenden analogen Sollspannungswert erzeugt, sowie einen Spannungsregler 5, dem eingangsseitig der analoge Sollspannungswert vom Digital/Analog-Wandler 4 zugeführt wird und der ausgangsseitig einen Ist-Spannungswert erzeugt, der die Versorgungsspannung der asynchronen Schaltung 2 bildet. Die Generatorschaltung 3 zur Erzeugung tatsächlicher Zufallszahlen umfaßt ihrerseits eine Rauschquelle 6, die eine Rauschspannung erzeugt, sowie einen von der Rauschquelle 6 angesteuerten Zufallszahlengenerator 7.

10

15

20

25

Anstelle der hier gezeigten Kombination der Rauschquelle 6 und des Zufallszahlengenerators 7 können jedoch beliebige andere Zufallsgeneratoren zum Erzeugen der Zufallszahlen als Eingangsgröße für den Digital/Analog-Wandler 4 verwendet werden.

30

35

Bei dem hier gezeigten bevorzugten Ausführungsbeispiel hat der Spannungsregler 5 ein Stellglied 8, eine Istwerterfassungsvorrichtung 9 und eine Differenzbildungsvorrichtung 10, deren Eingängen einerseits der analoge Sollspannungswert vom Digital/Analog-Wandler 4 und andererseits ein Ausgangssignal von der Istwerterfassungsvorrichtung 9 zugeführt werden.

Die Generatorschaltung 3, der Digital/Analog-Wandler 4 und der Spannungsregler 5 bilden miteinander eine Einrichtung zum

zufälligen zeitlichen Verändern der Versorgungsspannung bzw. einer Einrichtung zum Überlagern eines zufälligen zeitlichen Jitters über die Versorgungsspannung, mit der die asynchrone Schaltung 2 versorgt wird. Aufgrund der sich zufällig ändernden Versorgungsspannung kommt es zu einem zufälligen zeitlichen Jitter bei der Ausführung der Operationen in der asynchronen Schaltung, wodurch das Aufsynchronisieren der Einzelmessungen bei den sogenannten Side-Channel-Attacks verhindert oder zumindest erschwert wird.

Patentansprüche

1. Verfahren zum Verhindern des externen Erfassens von Operationen in einer integrierten Digitalschaltung (1), die eine
5 asynchrone Schaltung (2) aufweist,

mit dem Verfahrensschritt des zeitlichen Veränderns einer Versorgungsspannung der asynchronen Schaltung (2), um den Ausführungszeitpunkt von Operationen innerhalb der asynchronen Schaltung zeitlich zu verschieben.
10

2. Verfahren nach Anspruch 1, bei dem die zeitliche Veränderung der Versorgungsspannung in zufälliger Weise erfolgt.

15 3. Integrierte Digitalschaltung, mit
einer asynchronen Schaltung (2), und

einer Einrichtung (3, 4, 5) zum zeitlichen Verändern einer Versorgungsspannung der asynchronen Schaltung 2, um den Ausführungszeitpunkt von Operationen innerhalb der asynchronen Schaltung (2) zeitlich zu verschieben.
20

25 4. Integrierte Digitalschaltung nach Anspruch 3, bei der die Einrichtung (3, 4, 5) zum zeitlichen Verändern der Versorgungsspannung einen Zufallszahlengenerator (7) aufweist.

5. Integrierte Digitalschaltung nach Anspruch 4, bei der die Einrichtung (3, 4, 5) zum zeitlichen Verändern der Versorgungsspannung ferner eine Rauschspannungsquelle (6) aufweist, die den Zufallszahlengenerator (7) ansteuert.
30

6. Integrierte Digitalschaltung nach Anspruch 4 oder 5, bei der die Einrichtung (3, 4, 5) zum zeitlichen Verändern der Versorgungsspannung ferner einen Digital/Analog-Wandler (4) aufweist, der die vom Zufallszahlengenerator (7) erzeugten Digitalwerte in eine Analogspannung umwandelt.
35

7. Integrierte Digitalschaltung nach einem der Ansprüche 3 bis 6, bei der die Einrichtung (3, 4, 5) zum zeitlichen Verändern der Versorgungsspannung ferner einen Spannungsregler (5) aufweist.

8. Integrierte Digitalschaltung nach einem der Ansprüche 3 bis 7, bei der die asynchrone Schaltung (2) zur Ausführung eines Verschlüsselungsalgorithmus ausgebildet ist.

10

Zusammenfassung

Verhindern der unerwünschten externen Erfassung von Operationen in integrierten Digitalschaltungen

5

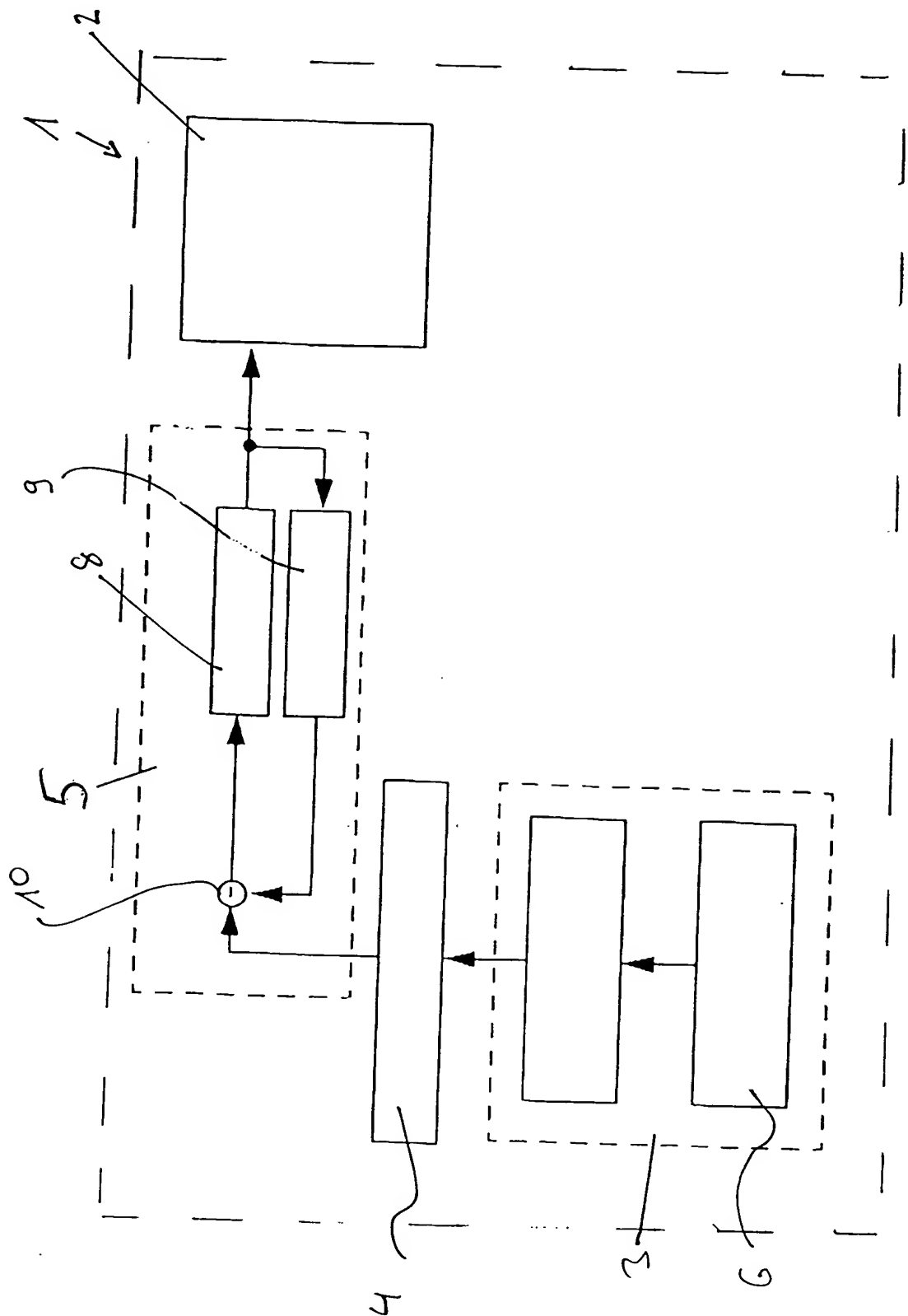
Bei einer Digitalschaltung (1), die eine asynchrone Schaltung (2) aufweist, wird die Versorgungsspannung der asynchronen Schaltung (2) mit einem Zufallsspannungsjitter variiert. Die zufällige Änderung der Versorgungsspannung bewirkt einen zeitlichen Jitter in der Abarbeitung der einzelnen Operationen innerhalb der asynchronen Schaltung, wodurch ein Aufsynchronisieren von Einzelmessungen bei Side-Channel-Attacks verhindert wird.

10

15

Figur

Figur zur Zusammenfassung



Bezugszeichenliste

- 1 Digitalschaltung
- 2 asynchrone Schaltung
- 3 Generatorschaltung
- 4 Digital/Analog-Wandler
- 5 Spannungsregler
- 6 Rauschquelle
- 7 Zufallszahlengenerator
- 8 Stellglied
- 9 Istwerterfassungsvorrichtung
- 10 Differenzbildungsvorrichtung

